



# SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、セキュア シェル (SSH) サーバ側でユーザ認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

- [機能情報の確認 \(1 ページ\)](#)
- [SSH 認証の X.509v3 証明書 の前提条件 \(2 ページ\)](#)
- [SSH 認証の X.509v3 証明書 の制約事項 \(2 ページ\)](#)
- [SSH 認証用の X.509v3 証明書に関する情報 \(2 ページ\)](#)
- [SSH 認証用の X.509v3 証明書の設定方法 \(3 ページ\)](#)
- [SSH 認証用の X.509v3 証明書の設定例 \(7 ページ\)](#)
- [に関する追加情報 SSH 認証の X.509v3 証明書 \(8 ページ\)](#)
- [SSH 認証の X.509v3 証明書 の機能情報 \(9 ページ\)](#)

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェアリリースのリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

## SSH 認証の X.509v3 証明書 の前提条件

- SSH 認証の X.509v3 証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。**ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

Warning: SSH command accepted but this CLI will be deprecated soon. Please move to new CLI "ip ssh server algorithm authentication". Please configure "default ip ssh server authenticate user" to make CLI ineffective.

- default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドを無効にします。その後、IOS セキュア シェル (SSH) サーバは **ip ssh server algorithm authentication** コマンドを使用して起動します。

## SSH 認証の X.509v3 証明書 の制約事項

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュア シェル (SSH) 側にのみ適用できます。
- IOS SSH サーバは、IOS SSH サーバ側のサーバおよびユーザ認証について、x509v3-ssh-rsa アルゴリズム ベースの証明書のみをサポートします。

## SSH 認証用の X.509v3 証明書に関する情報

### デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式 (RFC5280) のデジタル証明書は、アイデンティティの管理を実行するため使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタル アイデンティティがバインドされます。

公開キーインフラストラクチャ (PKI) のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局 (CA) 、さまざまなアイデンティティ パラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

### X.509v3 を使用したサーバおよびユーザ認証

サーバ認証の場合、IOS セキュア シェル (SSH) が確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル

(ssh-server-cert-profile-server コンフィギュレーションモード) で設定されたトラストポイントに関連付けられます。

ユーザ認証の場合、SSH クライアントが確認のためにユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル (ssh-server-cert-profile-user コンフィギュレーションモード) で設定された公開キーインフラストラクチャ (PKI) トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

## SSH 認証用の X.509v3 証明書の設定方法

### サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]}**
4. **ip ssh server certificate profile**
5. **server**
6. **trustpoint sign *PKI-trustpoint-name***
7. **ocsp-response include**
8. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable  Device# configure terminal	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	<b>ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa]   ssh-rsa [x509v3-ssh-rsa]}</b> 例：	ホストキー アルゴリズムの順序を定義します。セキュアシェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。

## ■ ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

	コマンドまたはアクション	目的
	Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa	(注) IOS SSH サーバには、1つ以上の設定済みホストキーアルゴリズムが必要です。 • ssh-rsa : 公開キーベース認証 • x509v3-ssh-rsa : 証明書ベース認証
ステップ 4	<b>ip ssh server certificate profile</b> 例 : Device(config)# ip ssh server certificate profile	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイルコンフィギュレーションモードを開始します。
ステップ 5	<b>server</b> 例 : Device(ssh-server-cert-profile)# server	サーバ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザコンフィギュレーションモードを開始します。
ステップ 6	<b>trustpoint sign PKI-trustpoint-name</b> 例 : Device(ssh-server-cert-profile-server)# trustpoint sign trust1	公開キーインフラストラクチャ (PKI) トラストポイントをサーバ証明書プロファイルにアタッチします。SSH サーバは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。
ステップ 7	<b>ocsp-response include</b> 例 : Device(ssh-server-cert-profile-server)# ocsp-response include	(任意) Online Certificate Status Protocol (OCSP) の応答または OCSP ステーリングをサーバ証明書と一緒に送信します。 (注) デフォルトではこのコマンドの「no」形式が設定されており、OCSP 応答はサーバ証明書と一緒に送信されません。
ステップ 8	<b>end</b> 例 : Device(ssh-server-cert-profile-server)# end	SSH サーバ証明書プロファイルのサーバコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

## ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm authentication {publickey | keyboard | password}**

4. **ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]}**
5. **ip ssh server certificate profile**
6. **user**
7. **trustpoint verify PKI-trustpoint-name**
8. **ocsp-response required**
9. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>ip ssh server algorithm authentication {publickey   keyboard   password}</b> 例： Device(config)# ip ssh server algorithm authentication publickey	ユーザ認証アルゴリズムの順序を定義します。セキュアシェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 <ul style="list-style-type: none"> <li>(注) IOS SSH サーバには、1つ以上の設定済みユーザ認証アルゴリズムが必要です。</li> <li>(注) ユーザ認証に証明書方式を使用するには、<b>publickey</b> キーワードを設定する必要があります。</li> <li>(注) <b>ip ssh server algorithm authentication</b> コマンドは <b>ip ssh server authenticate user</b> コマンドの代わりに使用します。</li> </ul>
ステップ 4	<b>ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa]   ssh-rsa [x509v3-ssh-rsa]}</b> 例： Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa	公開キーアルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。 <ul style="list-style-type: none"> <li>(注) IOS SSH クライアントには、1つ以上の設定済み公開キーアルゴリズムが必要です。               <ul style="list-style-type: none"> <li>• ssh-rsa : 公開キーベース認証</li> <li>• x509v3-ssh-rsa : 証明書ベース認証</li> </ul> </li> </ul>

## デジタル証明書を使用したサーバおよびユーザ認証の設定の確認

	コマンドまたはアクション	目的
ステップ 5	<b>ip ssh server certificate profile</b> 例： Device(config)# ip ssh server certificate profile	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイルコンフィギュレーションモードを開始します。
ステップ 6	<b>user</b> 例： Device(ssh-server-cert-profile)# user	ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザコンフィギュレーションモードを開始します。
ステップ 7	<b>trustpoint verify PKI-trustpoint-name</b> 例： Device(ssh-server-cert-profile-user)# trustpoint verify trust2	受信したユーザ証明書の確認に使用される公開キーインフラストラクチャ (PKI) トラストポイントを設定します。 (注) 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。
ステップ 8	<b>ocsp-response required</b> 例： Device(ssh-server-cert-profile-user)# ocsp-response required	(任意) 受信したユーザ証明書による Online Certificate Status Protocol (OCSP) の応答の有無を要求します。 (注) デフォルトではこのコマンドの「no」形式が設定されており、ユーザ証明書は OCSP 応答なしで受け入れられます。
ステップ 9	<b>end</b> 例： Device(ssh-server-cert-profile-user)# end	SSH サーバ証明書プロファイルのユーザコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

## デジタル証明書を使用したサーバおよびユーザ認証の設定の確認

## 手順の概要

1. **enable**
2. **show ip ssh**

## 手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

## ステップ2 show ip ssh

現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホストキー アルゴリズムであることを確認します。

例：

```
Device# show ip ssh

SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

---

## SSH 認証用の X.509v3 証明書の設定例

### 例：サーバ認証にデジタル証明書を使用するための IOS SSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

### 例：ユーザ認証用のユーザのデジタル証明書を確認するための IOSSSH サーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
```

```

Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end

```

## に関する追加情報 SSH 認証の X.509v3 証明書

### 関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	<a href="#">Cisco IOS Master Command List, All Releases</a>
セキュリティ コマンド	<ul style="list-style-type: none"> <li>『Cisco IOS Security Command Reference: Commands A to C』</li> <li>『Cisco IOS Security Command Reference: Commands D to L』</li> <li>『Cisco IOS Security Command Reference: Commands M to R』</li> <li>『Cisco IOS Security Command Reference: Commands S to Z』</li> </ul>
SSH 認証	『セキュア シェル コンフィギュレーション ガイド』の「セキュア シェル：ユーザ認証方式の設定」の章
公開キー インフラストラクチャ (PKI) のトラストポイント	『Public Key Infrastructure Configuration Guide』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

## シスコのテクニカルサポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス) 、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## SSH 認証の X.509v3 証明書 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 1: SSH 認証の X.509v3 証明書 の機能情報

機能名	リリース	機能情報
SSH 認証の X.509v3 証明書		<p>SSH 認証の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、セキュアシェル (SSH) サーバ側でユーザ認証を使用します。</p> <p>次のコマンドが導入または変更されました：<b>ip ssh server algorithm hostkey</b>、<b>ip ssh server algorithm authentication</b>、<b>ip ssh server certificate profile</b>。</p>

